

Exhibit 9

Redacted

[REDACTED]

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS**

SINGULAR COMPUTING LLC,

Plaintiff,

v.

GOOGLE LLC,

Defendant.

Civil Action No. 1:19-cv-12551 FDS

Hon. F. Dennis Saylor IV

**DECLARATION OF [REDACTED] IN SUPPORT OF OPPOSITION
TO PLAINTIFF'S MOTION TO COMPEL INSPECTION, TESTING, AND
SOURCE CODE OF THE ACCUSED PRODUCTS**

[REDACTED]

I, [REDACTED] declare and state as follows:

1. I am the Senior Site Facility Manager and Site Lead for Google's data-center site [REDACTED]. I have personal knowledge of the facts stated in this declaration, and if called as a witness, could and would testify to those facts.

2. I have been a Google employee for 14 years. As a Senior Site Facility Manager and Site Lead, I am responsible for the operation and maintenance of Google's data-center site [REDACTED]. I also have shared accountability with the Google Security team for the security of that site.

3. I understand that versions 2 and 3 of Google's TPUs (the "accused versions") have been accused of patent infringement by Singular Computing LLC ("Singular"), and that Singular has asked the Court to order an inspection of a Google data center with the accused versions installed and in use.


4. The [REDACTED] data center has the accused versions of TPUs installed and in use; however, neither the TPU boards nor the chips that are on them are visible by way of inspection—that is, by walking on the data-center floor. When in use in data centers, the TPU chips are covered by heat sinks and are a part of TPU boards. Those TPU boards are in housings and components in server racks. But the server racks in the data center are not labeled and an observer would not be able to determine whether they contain TPUs or some other hardware.

5. The data center also includes hardware and other infrastructure unrelated to TPUs, including intellectual property related to Google's highly secure networking, server, and facilities infrastructure. The data center also contains [REDACTED]

[REDACTED]



6. Google's data centers are some of the most sensitive and secure locations on any Google campus. Service continuity and data security are very important to Google's business and its customers. Google places tremendous value on the security, privacy, and reliability of its data centers, including the safeguards that comprise its security system. Any breach—physical or electronic—would impact the security of Google's systems, the privacy of its data (as well as its users' data), and the continuity of its services. Google promises its customers that only people with a strong business case or concern within Google will be allowed to enter Google's data-center sites.

7. For example, the  site includes multiple, layered safeguards spanning from alarms to biometric access points to laser-based intrusion detection. Every employee must walk through metal detectors and is subject to physical search in order to enter or exit the facilities. Google does not allow employees to use recording devices or cameras that do not belong to Google on premises, unless they receive authorization for a specific, limited business case. Google employs a "zero trust model" to limit electronic access or intrusion to the data center and data-center systems. The scope of data-center protections is explained in further detail in the following publicly available references:

- Google Data Center Security: 6 Layers Deep, (<https://www.youtube.com/watch?v=kd33UVZhnAA>);
- Google Data Centers: Data and Security, (<https://www.google.com/about/datacenters/data-security/>);
- Data Processing and Security Terms (Customers), (<https://cloud.google.com/terms/data-processing-terms>);



- Google Infrastructure Security Design Overview for Google Cloud, (https://cloud.google.com/security/infrastructure/design#operational_security); and
- Google Workspace security whitepaper, (<https://workspace.google.com/learn-more/security/security-whitepaper/page-4.html>).

8. There are also physical safety concerns with data center visits. Data center sites are industrial facilities with hazardous materials, high-voltage machinery, and high temperatures. Accordingly, there is significant opportunity for injury to people and to the machinery itself.

9. Google's concerns are not limited to unauthorized access or intrusion; the data centers need protection from a myriad of potential issues, including unintentional disclosures of sensitive, proprietary information by even well-meaning employees and visitors. We do not offer tours for Google employees or any external visitors. Less than one percent of Google employees will ever set foot in a Google data center, nearly all of whom are actually involved in data-center planning, operations, or security. Outside of regulatory audits, Google generally does not allow external visitors to Google's data centers. Google's concern with external visitors is not just with regard to the confidentiality of its intellectual property or competitive business practices. Any photographs or video recordings of the data center not authorized by Google could potentially reveal important security related information, such as the location of certain security equipment, equipment manufacturers, data-center layout, and Google's operational processes. The authorized pictures and videos of Google data-centers online have been reviewed and curated to remove sensitive information about Google's security set-up and to ensure that no intellectual property is exposed.

10. Coordinating data center visits also poses a high risk of business interruption and would be a significant burden. Due to the highly secure nature of a data-center site, we generally

[REDACTED]

operate with a limited number of employees who have security clearance. Only essential employees are generally allowed onto the data-center floor. In addition, the data centers are

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Thus, if Google were required to allow external visitors in connection with this litigation, that would result in substantial business disruption as we would need significant time and employee resources to prepare for such a visit. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

11. Google policies also require that all individuals entering a data center receive the same mandatory safety and security training that data-center employees receive before being allowed access to a data-center floor. We would have to coordinate a one-off training for any visitors. Google also requires all individuals entering a data center to review, sign, and abide by the conditions set forth in the data-center rules and data-center non-disclosure agreements. To protect against even inadvertent disclosure, Google's policies require that visitors do not take photographs or video recordings on non-Google owned devices, especially because Google's

[REDACTED]

publicly available materials--which have been vetted for these concerns--could substitute for any independent efforts to take photographs.

12. Google's other requirements for entry into a data-center site depend on the circumstances of that entry and the scope and length of any potential inspection. I understand that Singular has not provided specific parameters; without those parameters, I cannot immediately ascertain what other measures would be necessary to address the high risk of further business disruption.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.

Executed on August 6, 2021 at [REDACTED]

[REDACTED]



CERTIFICATE OF SERVICE

I certify that this document is being filed through the Court's electronic filing system, which serves counsel for other parties who are registered participants as identified on the Notice of Electronic Filing (NEF). Any counsel for other parties who are not registered participants are being served by first class mail on the date of electronic filing.

/s/ Nathan R. Speed
Nathan R. Speed